特 許 協 力 条 約

ＰＣＴ

特許性に関する国際予備報告（特許協力条約第二章）

（法第 12 条、法施行規則第 56 条）
〔ＰＣＴ36 条及びＰＣＴ規則 70〕

出願人又は代理人 の書類記号 JJVC-146-PCT	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００５／００１２１１	国際出願日 （日．月．年） ２８．０１．２００５	優先日 （日．月．年） ３０．０１．２００４
国際特許分類（ＩＰＣ） Int.Cl. *G06F7/58 (2006.01), H03K3/84 (2006.01)*		
出願人（氏名又は名称） 日本ビクター株式会社		

１．この報告書は、ＰＣＴ35 条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第 57 条（ＰＣＴ36 条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で ３ ページからなる。

３．この報告には次の附属物件も添付されている。

ａ．☑ 附属書類は全部で 7 ページである。

☑ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則 70.16 及び実施細則第 607 号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

ｂ．☐ 電子媒体は全部で ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ （電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。
（実施細則第 802 号参照）

４．この国際予備審査報告は、次の内容を含む。

☑ 第Ｉ欄 国際予備審査報告の基礎
☐ 第Ⅱ欄 優先権
☐ 第Ⅲ欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐ 第Ⅳ欄 発明の単一性の欠如
☑ 第Ⅴ欄 ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄 ある種の引用文献
☐ 第Ⅶ欄 国際出願の不備
☐ 第Ⅷ欄 国際出願に対する意見

国際予備審査の請求書を受理した日 ３０．１１．２００５	国際予備審査報告を作成した日 ２５．０５．２００６
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｅ ２９５１ 中田 剛史 電話番号 ０３－３５８１－１１０１ 内線 ３５２１

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００５年４月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１２１１

第Ⅰ欄　報告の基礎

１．言語に関し、この予備審査報告は以下のものを基礎とした。

☑ 出願時の言語による国際出願

☐ 出願時の言語から次の目的のための言語である＿＿＿＿＿＿ 語に翻訳された、この国際出願の翻訳文

☐ 国際調査（ＰＣＴ規則12.3(a)及び23.1(b)）

☐ 国際公開（ＰＣＴ規則12.4(a)）

☐ 国際予備審査（ＰＣＴ規則55.2(a)又は55.3(a)）

２．この報告は下記の出願書類を基礎とした。（法第6条（ＰＣＴ14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☑ 明細書

第 １，６－１４ ページ、出願時に提出されたもの

第 ２－５ ページ*、３０．１１．２００５ 付けで国際予備審査機関が受理したもの

第＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 請求の範囲

第＿＿＿＿＿＿ 項、出願時に提出されたもの

第＿＿＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの

第 １－４ 項*、３０．１１．２００５ 付けで国際予備審査機関が受理したもの

第＿＿＿＿＿＿ 項*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 図面

第 １－９ ~~ページ／~~図 、出願時に提出されたもの

第＿＿＿＿＿＿ ページ／図*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

第＿＿＿＿＿＿ ページ／図*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

３．☐ 補正により、下記の書類が削除された。

☐ 明細書　第＿＿＿＿＿＿ ページ

☐ 請求の範囲　第＿＿＿＿＿＿ 項

☐ 図面　第＿＿＿＿＿＿ ページ／図

☐ 配列表（具体的に記載すること）＿＿＿＿＿＿

☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

４．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則 70.2(c)）

☐ 明細書　第＿＿＿＿＿＿ ページ

☐ 請求の範囲　第＿＿＿＿＿＿ 項

☐ 図面　第＿＿＿＿＿＿ ページ／図

☐ 配列表（具体的に記載すること）＿＿＿＿＿＿

☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

＊ ４．に該当する場合、その用紙に〝superseded〟と記入されることがある。

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００１２１１

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）	請求の範囲	１－４	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲		有
	請求の範囲	１－４	無
産業上の利用可能性（ＩＡ）	請求の範囲	１－４	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：
ＪＰ　９－１７９７２６　Ａ（日本電気株式会社）１９９７．０７．１１，全文、全図&ＥＰ　７８２０６９　Ａ１
文献２：
ＪＰ　１１－２３４０９６　Ａ（富士通株式会社）１９９９．０８．２７，全文、全図&ＥＰ　９３８１９２　Ａ２&ＵＳ　６２７５５２０　Ｂ１
文献３：
ＪＰ　６１－１４１２３１　Ａ（ソニー株式会社）１９８６．０６．２８，全文、全図（ファミリー無し）
文献４：
ＪＰ　２００１－２７４７８７　Ａ（日本ビクター株式会社）２００１．１０．０５，全文、全図（ファミリー無し）
文献５：
ＪＰ　２００１－２７４７８６　Ａ（日本ビクター株式会社）２００１．１０．０５，全文、全図&ＥＰ　１１１９１３１　Ａ２&ＵＳ　６９７５７３０　Ｂ１
文献６：
ＪＰ　２－４３５９４　Ａ（松下電器産業株式会社）１９９０．０２．１４，全文、全図（ファミリー無し）

請求の範囲１－４：
国際調査報告で引用された文献１乃至文献３、及び新たに引用した文献４乃至文献６により進歩性を有しない。
文献３には、所定の識別記号によって特性多項式を指定することが、文献４及び文献５には、イニシャルデータの通信を行うことが、文献６には、出力が論理演算される各ＬＦＳＲの特性多項式を、特性多項式の一種である原始多項式で構成することが記載されており、文献１または文献２に記載されたような、従来周知の乱数生成装置に当該機構を採用することは当業者にとって容易である。

たとえ非線形な処理を組み合わせた方法であっても、ある特定のアルゴリズムで擬似乱数が生成されるため、初期値や生成される擬似乱数列の一部からその後生成される擬似乱数が推測される恐れがあった。

[0006] また、複数の線形フィードバックシフトレジスタからいくつかのレジスタを選択して擬似乱数を生成する場合には、生成される擬似乱数列の推測は困難になるものの、任意の係数を特性多項式とする線形フィードバックシフトレジスタを組み合わせると、生成される擬似乱数列が必ずしもM系列(Maximum length sequences)とはならずに、短い周期で同じ擬似乱数列を繰り返し生成してしまうという問題があるため、予め特定の条件を満たす多項式を多数用意した中から選択して組み合わせる必要があった。これは実際の処理では、常に利用するわけではない線形フィードバックシフトレジスタを実装する必要があり効率的ではなかった。

発明の開示

[0007] 本発明は、生成される擬似乱数列や送受信されるデータを観測されても、その後生成される擬似乱数列の推測が困難な暗号通信に好適な擬似乱数生成装置および擬似乱数生成プログラムを提供することを目的とする。

[0008] 上記目的を達成するため、第1の態様に係る発明は、所定のビット長の擬似乱数列を生成する擬似乱数生成装置であって、m段のシフトレジスタを有し、特定多項式として原始多項式を用い、前記m段のシフトレジスタに第1の初期値と第1の係数を設定して所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタと、n段のシフトレジスタを有し、特定多項式を用い、前記n段のシフトレジスタに第2の初期値と第2の係数を設定して所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタと、所定の条件に従って、前記第1および第2の初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタおよび前記第2の線形フィードバックシフトレジスタへ供給する初期値生成部と、所定の条件に従って、前記第2の線形フィードバックシフトレジスタで用いる前記第2の係数を生成し、前記第2の線形フィードバックシフトレジスタへ供給する多項式係数生成部と、前記第1の線形フィードバックシフトレジスタで用いる原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶部と、

所定の条件に従って、前記原始多項式記憶部に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択部と、前記第１の線形フィードバックシフトレジスタから出力されるビット列と、前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力部と、を備える擬似乱数生成装置を要旨とする。

[0009] また、第２の態様に係る発明は、第１の態様に係る発明において、前記擬似乱数生成装置は、前記原始多項式選択部によって選択された前記原始多項式の識別情報、前記初期値生成部によって生成された前記第１および第２の初期値、前記多項式係数生成部によって生成された前記第２の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１および第２の初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記第２の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択部に供給する通信部を備え、前記原始多項式選択部は、前記通信部によって抽出された前記識別情報を基に、前記原始多項式記憶部に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の係数として前記第１の線形フィードバックシフトレジスタへ供給することを要旨とする。

[0010] また、上記目的を達成するため、第３の態様に係る発明は、コンピュータによって所定のビット長の擬似乱数列を生成する処理を実行させる擬似乱数生成プログラムであって、当該擬似乱数生成プログラムは、前記コンピュータを、m段のシフトレジスタを有し、特定多項式として原始多項式を用い、前記m段のシフトレジスタに第１の初期値と第１の係数を設定して所定のビット長のビット列を出力する第１の線形フィードバックシフトレジスタと、n段のシフトレジスタを有し、特定多項式を用い、前記n段のシフトレジスタに第２の初期値と第２の係数を設定して所定のビット長のビ

ット列を出力する第２の線形フィードバックシフトレジスタと、所定の条件に従って、前記第１および第２の初期値を生成し、それぞれの当該初期値を前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタへ供給する初期値生成手段と、所定の条件に従って、前記第２の線形フィードバックシフトレジスタで用いる前記第２の係数を生成し、前記第２の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、前記第１の線形フィードバックシフトレジスタで用いる原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶手段と、所定の条件に従って、前記原始多項式記憶部に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、前記第１の線形フィードバックシフトレジスタから出力されるビット列と、前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段として機能させる擬似乱数生成プログラムを要旨とする。

[0011] また、第４の態様に係る発明は、第３の態様に係る発明において、前記擬似乱数生成プログラムは、前記コンピュータを前記原始多項式選択手段によって選択された前記原始多項式の識別情報、前記初期値生成手段によって生成された前記第１および第２の初期値、前記多項式係数生成手段によって生成された前記第２の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１および第２の初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記第２の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、前記原始多項式選択手段は、前記通信手段によって抽出された前記識別情報を基に、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記

第１の係数として前記第１の線形フィードバックシフトレジスタへ供給することを要旨とする。

図面の簡単な説明

[0012] ［図１］図１は、第１の実施形態における擬似乱数生成装置の機能構成を示す図である。

［図２］図２は、第１線形フィードバックシフトレジスタの回路構成を示す図である。

［図３］図３は、第２線形フィードバックシフトレジスタの回路構成を示す図である。

［図４］図４は、第１の実施形態における擬似乱数生成の処理を示すフローチャートである。

［図５］図５は、第１線形フィードバックシフトレジスタと第２線形フィードバックシフトレジスタの値の遷移を示す図である。

［図６］図６は、第２の実施形態における擬似乱数生成装置の機能構成を示す図である。

［図７］図７は、第２の実施形態における擬似乱数生成の処理を示すフローチャートである。

［図８］図８は、第３の実施形態における擬似乱数生成装置の機能構成を示す図である。

［図９］図９は、第３の実施形態における擬似乱数生成の処理を示すフローチャートである。

発明を実施するための最良の形態

[0013] 本発明の実施形態を、図１～図９を用いて説明する。なお、擬似乱数生成装置１が生成する擬似乱数のビット長をｈ＋１とする。

[0014] ＜第１の実施形態＞

第１の実施形態における擬似乱数生成装置１Ａは、図１に示すように、第１線形フィードバックシフトレジスタ２、第２線形フィードバックシフトレジスタ３、初期値生成部４、多項式係数生成部５、および擬似乱数出力部６を有する。

[0015] 第１線形フィードバックシフトレジスタ２は、ｍ次の線形フィードバックシフトレジスタであり、ｍ個のフリップフロップ回路を有する（詳細については後述）。また、第２線形

請求の範囲

[1] （補正後）所定のビット長の擬似乱数列を生成する擬似乱数生成装置（1）であって、

m段のシフトレジスタを有し、特定多項式として原始多項式を用い、前記m段のシフトレジスタに第1の初期値と第1の係数を設定して所定のビット長のビット列を出力する第1の線形フィードバックシフトレジスタ（2）と、

n段のシフトレジスタを有し、特定多項式を用い、前記n段のシフトレジスタに第2の初期値と第2の係数を設定して所定のビット長のビット列を出力する第2の線形フィードバックシフトレジスタ（3）と、

所定の条件に従って、前記第1および第2の初期値を生成し、それぞれの当該初期値を前記第1の線形フィードバックシフトレジスタ（2）および前記第2の線形フィードバックシフトレジスタ（3）へ供給する初期値生成部（4）と、

所定の条件に従って、前記第2の線形フィードバックシフトレジスタ（3）で用いる前記第2の係数を生成し、前記第2の線形フィードバックシフトレジスタ（3）へ供給する多項式係数生成部（5）と、

前記第1の線形フィードバックシフトレジスタ（2）で用いる原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶部（8）と、

所定の条件に従って、前記原始多項式記憶部（8）に記憶されている原始多項式を1つ選択し、その原始多項式の係数を前記第1の係数として前記第1の線形フィードバックシフトレジスタ（2）へ供給する原始多項式選択部（7）と、

前記第1の線形フィードバックシフトレジスタ（2）から出力されるビット列と、前記第2の線形フィードバックシフトレジスタ（3）から出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力部（6）と、

を備えることを特徴とする擬似乱数生成装置（1）。

[2] （補正後）前記擬似乱数生成装置（1C）は、

前記原始多項式選択部（7）によって選択された前記原始多項式の識別情報、前記初期値生成部（4）によって生成された前記第1および第2の初期値、前記多項式係数生成部（5）によって生成された前記第2の係数のそれぞれからなるイニシャルデータを生成し、

当該イニシャルデータを他の擬似乱数生成装置（１Ｃ）へ送出し、当該イニシャルデータを他の擬似乱数生成装置（１Ｃ）から受信した場合は、当該イニシャルデータから前記第１および第２の初期値を抽出して前記第１の線形フィードバックシフトレジスタ（２）と前記第２の線形フィードバックシフトレジスタ（３）に供給し、当該イニシャルデータから前記第２の係数を抽出して前記第２の線形フィードバックシフトレジスタ（３）へ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択部（７）に供給する通信部（９）を備え、

前記原始多項式選択部（７）は、前記通信部（９）によって抽出された前記識別情報を基に、前記原始多項式記憶部（８）に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の係数として前記第１の線形フィードバックシフトレジスタ（２）へ供給することを特徴とする請求の範囲第１項に記載の擬似乱数生成装置。

［３］ （補正後）コンピュータによって所定のビット長の擬似乱数列を生成する処理を実行させる擬似乱数生成プログラムであって、

当該擬似乱数生成プログラムは、前記コンピュータを、

ｍ段のシフトレジスタを有し、特定多項式として原始多項式を用い、前記ｍ段のシフトレジスタに第１の初期値と第１の係数を設定して所定のビット長のビット列を出力する第１の線形フィードバックシフトレジスタと、

ｎ段のシフトレジスタを有し、特定多項式を用い、前記ｎ段のシフトレジスタに第２の初期値と第２の係数を設定して所定のビット長のビット列を出力する第２の線形フィードバックシフトレジスタと、

所定の条件に従って、前記第１および第２の初期値を生成し、それぞれの当該初期値を前記第１の線形フィードバックシフトレジスタおよび前記第２の線形フィードバックシフトレジスタへ供給する初期値生成手段と、

所定の条件に従って、前記第２の線形フィードバックシフトレジスタで用いる前記第２の係数を生成し、前記第２の線形フィードバックシフトレジスタへ供給する多項式係数生成手段と、

前記第１の線形フィードバックシフトレジスタで用いる原始多項式を、前記原始多項式を指定する識別情報と共に複数記憶する原始多項式記憶手段と、

所定の条件に従って、前記原始多項式記憶部に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の係数として前記第１の線形フィードバックシフトレジスタへ供給する原始多項式選択手段と、

前記第１の線形フィードバックシフトレジスタから出力されるビット列と、前記第２の線形フィードバックシフトレジスタから出力されるビット列とに基づいて、各ビットの論理演算から所定のビット長の擬似乱数列を生成し、出力する擬似乱数出力手段と、

して機能させることを特徴とする擬似乱数生成プログラム。

［４］　（補正後）前記擬似乱数生成プログラムは、前記コンピュータを

前記原始多項式選択手段によって選択された前記原始多項式の識別情報、前記初期値生成手段によって生成された前記第１および第２の初期値、前記多項式係数生成手段によって生成された前記第２の係数のそれぞれからなるイニシャルデータを生成し、当該イニシャルデータを他の擬似乱数生成装置へ送出し、当該イニシャルデータを他の擬似乱数生成装置から受信した場合は、当該イニシャルデータから前記第１および第２の初期値を抽出して前記第１の線形フィードバックシフトレジスタと前記第２の線形フィードバックシフトレジスタに供給し、当該イニシャルデータから前記第２の係数を抽出して前記第２の線形フィードバックシフトレジスタへ供給し、当該イニシャルデータから前記原始多項式の識別情報を抽出して前記原始多項式選択手段に供給する通信手段としても機能させ、

前記原始多項式選択手段は、前記通信手段によって抽出された前記識別情報を基に、前記原始多項式記憶手段に記憶されている原始多項式を１つ選択し、その原始多項式の係数を前記第１の係数として前記第１の線形フィードバックシフトレジスタへ供給する手段であることを特徴とする請求の範囲第３項に記載の擬似乱数生成プログラム。